MC

0460
6-13-01

PATENT #2
81942.0015

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of:

KATAYANAGI, et al.

Serial No: 09/862,888

Filed: May 21, 2001

For: Encryption Method, Decryption Method, Cryptographic Communication Method, Cryptographic Communication System, Memory Product and Data Signal Embodied in Carrier Wave

Art Unit: Not Assigned

Examiner: Not Assigned

I hereby certify that this correspondence is being deposited with the United States Postal Service with sufficient postage as first class mail in an envelope addressed to:
Assistant Commissioner for Patents
Washington D.C. 20231, on
June 18, 2001
Date of Deposit
Michael Crapenhoft, Reg. No. 37,115
Name
Signature June 18, 2001
Date

TRANSMITTAL OF PRIORITY DOCUMENT

Assistant Commissioner for Patents
Washington, D.C. 20231

Dear Sir:

Enclosed herewith is a certified copy of Japanese patent application No. 2001-097701 which was filed March 29, 2001, from which priority is claimed under 35 U.S.C. § 119 and Rule 55.

Acknowledgment of the priority document(s) is respectfully requested to ensure that the subject information appears on the printed patent.

Respectfully submitted,

HOGAN & HARTSON L.L.P.

Date: June 18, 2001

By: _____
Michael Crapenhoft
Registration No. 37,115
Attorney for Applicant(s)

500 South Grand Avenue, Suite 1900
Los Angeles, California 90071
Telephone: 213-337-6700
Facsimile: 213-337-6701

日本国特許庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office

出願年月日
Date of Application: ２００１年　３月２９日

出願番号
Application Number: 特願２００１－０９７７０１

出願人
Applicant(s): 村田機械株式会社
笠原　正雄

CERTIFIED COPY OF PRIORITY DOCUMENT

２００１年　５月１１日

特許庁長官
Commissioner,
Japan Patent Office

及川耕造

出証番号　出証特２００１－３０４０４９１

【書類名】　特許願

【整理番号】　21931

【提出日】　平成13年 3月29日

【あて先】　特許庁長官殿

【国際特許分類】　G09C 1/00

H04K 1/00

【発明の名称】　暗号化方法，復号方法，暗号通信方法，暗号通信システム，コンピュータプログラム及び記録媒体

【請求項の数】　30

【発明者】

【住所又は居所】　滋賀県大津市仰木の里東８丁目７－１２

【氏名】　片柳　磨子

【発明者】

【住所又は居所】　京都府京都市伏見区竹田向代町１３６番地　村田機械株式会社　本社工場内

【氏名】　村上　恭通

【発明者】

【住所又は居所】　大阪府箕面市粟生外院４丁目１５番３号

【氏名】　笠原　正雄

【特許出願人】

【識別番号】　000006297

【氏名又は名称】　村田機械株式会社

【代表者】　村田　純一

【特許出願人】

【識別番号】　597008636

【氏名又は名称】　笠原　正雄

【代理人】

【識別番号】　100078868

【弁理士】

【氏名又は名称】　河野　登夫

【電話番号】　06-6944-4141

【選任した復代理人】

【識別番号】　100114557

【弁理士】

【氏名又は名称】　河野　英仁

【電話番号】　06-6944-4141

【先の出願に基づく優先権主張】

【出願番号】　特願2000-153358

【出願日】　平成12年 5月24日

【先の出願に基づく優先権主張】

【出願番号】　特願2000-307822

【出願日】　平成12年10月 6日

【手数料の表示】

【予納台帳番号】　001889

【納付金額】　21,000円

【提出物件の目録】

【物件名】　明細書　1

【物件名】　図面　1

【物件名】　要約書　1

【包括委任状番号】　9805283

【プルーフの要否】　要

【書類名】　明細書

【発明の名称】　暗号化方法，復号方法，暗号通信方法，暗号通信システム，コンピュータプログラム及び記録媒体

【特許請求の範囲】

【請求項１】　平文から暗号文を得る暗号化方法において、暗号化すべき平文を分割してなる複数の成分を有する平文ベクトルに複数の任意の乱数を成分とする乱数ベクトルを加えた合成ベクトルと、公開されている公開ベクトルとを用いて暗号文を得ることを特徴とする暗号化方法。

【請求項２】　前記合成ベクトルの成分と前記公開ベクトルの成分との積和演算結果を法で割った剰余を暗号文とする請求項１に記載の暗号化方法。

【請求項３】　平文から暗号文を得る暗号化方法において、暗号化すべき平文をｋ分割してなるｋ個の成分を有する第１ベクトルにｎ個の任意の乱数を成分とする第２ベクトルを加えた（ｋ＋ｎ）個の成分を有する第３ベクトルと、整数d_i（$1 \leqq i \leqq k+n$）を用いて（ｋ＋ｎ）個の各成分D_iが$D_i = d / d_i$（但し、$d = d_1\ d_2 \cdots d_{k+n}$）に設定された第４ベクトルとを用いて暗号文を得ることを特徴とする暗号化方法。

【請求項４】　平文から暗号文を得る暗号化方法において、暗号化すべき平文をｋ分割してなるｋ個の成分を有する第１ベクトルにｎ個の任意の乱数を成分とする第２ベクトルを加えた（ｋ＋ｎ）個の成分を有する第３ベクトルと、整数d_i（$1 \leqq i \leqq k+n$）及び乱数v_iを用いて（ｋ＋ｎ）個の各成分V_iが$V_i = (d / d_i) \cdot v_i$（但し、$d = d_1\ d_2 \cdots d_{k+n}$）に設定された第４ベクトルとを用いて暗号文を得ることを特徴とする暗号化方法。

【請求項５】　平文から暗号文を得る暗号化方法において、暗号化すべき平文をｋ分割してなるｋ個の成分を有する第１ベクトルにｎ個の任意の乱数を成分とする第２ベクトルを加えた（ｋ＋ｎ）個の成分を有する第３ベクトルと、Ｌ組（$L \geqq 2$）の整数$d_i^{(y)}$（$1 \leqq i \leqq k+n$，$1 \leqq y \leqq L$）を用いて各組毎に（ｋ＋ｎ）個の各成分$D_i^{(y)}$が$D_i^{(y)} = d^{(y)} / d_i^{(y)}$（但し、$d^{(y)} = d_1^{(y)}\ d_2^{(y)} \cdots d_{k+n}^{(y)}$）に設定されたＬ組の第４ベクトルとを用いて暗号文を得ることを特徴とする暗号化方法。

【請求項６】　平文から暗号文を得る暗号化方法において、暗号化すべき平文をｋ分割してなるｋ個の成分を有する第１ベクトルにｎ個の任意の乱数を成分とする第２ベクトルを加えた（ｋ＋ｎ）個の成分を有する第３ベクトルと、Ｌ組（Ｌ≧２）の整数$d_i^{(y)}$（$1 \leqq i \leqq k+n$，$1 \leqq y \leqq L$）及び乱数$v_i^{(y)}$を用いて各組毎に（ｋ＋ｎ）個の各成分$V_i^{(y)}$が$V_i^{(y)} = (d^{(y)} / d_i^{(y)}) \cdot v_i^{(y)}$（但し、$d^{(y)} = d_1^{(y)} d_2^{(y)} \cdots d_{k+n}^{(y)}$）に設定されたＬ組の第４ベクトルとを用いて暗号文を得ることを特徴とする暗号化方法。

【請求項７】　$gcd(V_i, d_i) = 1$を満たす請求項４に記載の暗号化方法。

【請求項８】　$gcd(V_i^{(y)}, d_i^{(y)}) = 1$を満たす請求項６に記載の暗号化方法。

【請求項９】　$gcd(d_i^{(y)}, d_j^{(y)}) = 1$（$1 \leqq j \leqq k+n$）を満たす請求項６または８に記載の暗号化方法。

【請求項１０】　前記第３ベクトルの各成分と、前記第４ベクトルを基にモジュラ変換した公開鍵ベクトルの各成分とによる積和演算に基づいて暗号文を得るようにした請求項３～９の何れかに記載の暗号化方法。

【請求項１１】　平文から暗号文を得る暗号化方法において、暗号化すべき平文を分割してなるｋ個の成分を有する第１ベクトル、ｎ個の任意の乱数を成分とする第２ベクトル、及び、前記ｋ個の成分または前記ｎ個の成分の位置を特定する情報を示すｈ個の成分を有する第３ベクトルを加えたＫ（＝ｋ＋ｎ＋ｈ）個の成分を有する第４ベクトルと、公開されている第５ベクトルとを用いて暗号文を得ることを特徴とする暗号化方法。

【請求項１２】　前記暗号文は、前記第４ベクトルと前記第５ベクトルとを用いて得られる複数のブロックから構成されており、各ブロックにおいて、前記第４ベクトルにおける前記ｈ個の成分の位置は同一である請求項１１に記載の暗号化方法。

【請求項１３】　前記暗号文は、前記第４ベクトルと前記第５ベクトルとを用いて得られる複数のブロックから構成されており、前のブロックでの前記ｋ個の成分に応じて次のブロックでの前記第４ベクトルにおける前記ｋ個の成分また

は前記ｎ個の成分の位置を決定する請求項１１に記載の暗号化方法。

【請求項１４】　前記暗号文は、前記第４ベクトルと前記第５ベクトルとを用いて得られる１つのブロックと、前記第３ベクトルのｈ個の成分を平文を分割してなるｈ個の成分に置き換えた前記第４ベクトルと前記第５ベクトルとを用いて得られる複数のブロックとから構成されており、前のブロックでの平文を分割してなる前記ｋ個または（ｋ＋ｈ）個の成分に応じて次のブロックでの前記第４ベクトルにおける（ｋ＋ｈ）個の成分または前記ｎ個の成分の位置を決定する請求項１１に記載の暗号化方法。

【請求項１５】　前記第５ベクトルは、整数d_i（$1 \leqq i \leqq K$）を用いて各成分D_iが$D_i = (d / d_i)$（但し、$d = d_1\ d_2 \cdots d_K$）に設定された第６ベクトルとを用いて生成する請求項１１～１４の何れかに記載の暗号化方法。

【請求項１６】　前記第５ベクトルは、整数d_i（$1 \leqq i \leqq K$）及び乱数v_iを用いて各成分V_iが$V_i = (d / d_i) \cdot v_i$（但し、$d = d_1\ d_2 \cdots d_K$）に設定された第６ベクトルとを用いて生成する請求項１１～１４の何れかに記載の暗号化方法。

【請求項１７】　前記第５ベクトルは、Ｌ組（$L \geqq 2$）の整数$d_i^{(y)}$（$1 \leqq i \leqq K$，$1 \leqq y \leqq L$）を用いて各組毎にＫ個の各成分$D_i^{(y)}$が$D_i^{(y)} = d^{(y)} / d_i^{(y)}$（但し、$d^{(y)} = d_1^{(y)}\ d_2^{(y)} \cdots d_K^{(y)}$）に設定されたＬ組の第６ベクトルとを用いて生成する請求項１１～１４の何れかに記載の暗号化方法。

【請求項１８】　前記第５ベクトルは、Ｌ組（$L \geqq 2$）の整数$d_i^{(y)}$（$1 \leqq i \leqq k+n$，$1 \leqq y \leqq L$）及び乱数$v_i^{(y)}$を用いて各組毎にＫ個の各成分$V_i^{(y)}$が$V_i^{(y)} = (d^{(y)} / d_i^{(y)}) \cdot v_i^{(y)}$（但し、$d^{(y)} = d_1^{(y)}\ d_2^{(y)} \cdots d_K^{(y)}$）に設定されたＬ組の第６ベクトルとを用いて生成する請求項１１～１４の何れかに記載の暗号化方法。

【請求項１９】　$gcd(V_i, d_i) = 1$を満たす請求項１６に記載の暗号化方法。

【請求項２０】　$gcd(V_i^{(y)}, d_i^{(y)}) = 1$を満たす請求項１８に記載の暗号化方法。

【請求項２１】　ｇｃｄ（$d_i^{(y)}$，$d_j^{(y)}$）＝１（１≦ｊ≦Ｋ）を満たす請求項１８または２０に記載の暗号化方法。

【請求項２２】　前記第４ベクトルの各成分と、前記第６ベクトルを基にモジュラ変換した前記第５ベクトルの各成分とによる積和演算に基づいて暗号文を得るようにした請求項１５～２１の何れかに記載の暗号化方法。

【請求項２３】　請求項１～１０の何れかに記載の暗号化方法を用いて得られた暗号文を復号する復号方法であって、前記平文ベクトルまたは前記第１ベクトルの成分を、前記乱数ベクトルまたは前記第２ベクトルの成分とは独立的に復号することを特徴とする復号方法。

【請求項２４】　請求項１～２または１１～２１の何れかに記載の暗号化方法を用いて得られた暗号文を復号する復号方法であって、前記平文ベクトルまたは前記第１ベクトルの成分の位置を同定しながら、前記暗号文を平文に復号することを特徴とする復号方法。

【請求項２５】　第１のエンティティ側で、請求項１に記載の暗号化方法に従って平文から暗号文を作成して第２のエンティティ側へ伝送し、伝送された暗号文を該第２のエンティティ側で平文に復号することにより、エンティティ間で情報の通信を行う暗号通信方法であって、前記合成ベクトルにおける前記平文ベクトルの成分または前記乱数ベクトルの成分の位置を前記第１のエンティティ側で設定し、その設定した位置を示す情報を前記第２のエンティティ側へ報知することを特徴とする暗号通信方法。

【請求項２６】　前記設定した位置を示す情報を、作成する暗号文に盛り込んで前記第２のエンティティ側へ伝送する請求項２５に記載の暗号通信方法。

【請求項２７】　第１のエンティティ側で、請求項１に記載の暗号化方法に従って平文から暗号文を作成して第２のエンティティ側へ伝送し、伝送された暗号文を該第２のエンティティ側で平文に復号することにより、エンティティ間で情報の通信を行う暗号通信方法であって、前記合成ベクトルにおける前記平文ベクトルの成分または前記乱数ベクトルの成分の位置を前記第２のエンティティ側で設定し、その設定した位置を示す情報を前記第１のエンティティ側へ報知することを特徴とする暗号通信方法。

【請求項２８】　両エンティティ間で暗号文による情報通信を行う暗号通信システムにおいて、請求項１～２２の何れかに記載の暗号化方法を用いて平文から暗号文を作成する暗号化器と、作成した暗号文を第１のエンティティから第２のエンティティへ送信する通信路と、送信された暗号文から平文を復号する復号器とを備えることを特徴とする暗号通信システム。

【請求項２９】　コンピュータに、平文から積和型の暗号文を得ることを実行させるためのコンピュータプログラムにおいて、暗号化すべき平文を分割してなる複数の成分を有する平文ベクトルに複数の任意の乱数を成分とする乱数ベクトルを加えて合成ベクトルを得る手順と、該合成ベクトルと公開されている公開ベクトルとを用いて暗号文を得る手順とを、コンピュータに実行させることを特徴とするコンピュータプログラム。

【請求項３０】　コンピュータに、平文から積和型の暗号文を得させるためのコンピュータプログラムを記録してあるコンピュータでの読み取りが可能な記録媒体において、暗号化すべき平文を分割してなる複数の成分を有する平文ベクトルに複数の任意の乱数を成分とする乱数ベクトルを加えた合成ベクトルを得ることをコンピュータに実行させるプログラムコード手段と、該合成ベクトルと公開されている公開ベクトルとを用いて暗号文を得ることをコンピュータに実行させるプログラムコード手段とを含むコンピュータプログラムを記録してあることを特徴とする記録媒体。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は、公開鍵を用いて平文を暗号文に変換する公開鍵暗号系に関し、特に、積和型の暗号文を作成する暗号化方法、その暗号化方法にて得られた暗号文を復号する復号方法、その暗号化方法を利用する暗号通信方法及び暗号通信システム、並びに、その暗号化方法を実施するためのコンピュータプログラム及び記録媒体に関する。

【０００２】

【従来の技術】

高度情報化社会と呼ばれる現代社会では、コンピュータネットワークを基盤として、ビジネス上の重要な文書・画像情報が電子的な情報という形で伝送通信されて処理される。このような電子情報は、容易に複写が可能である、複写物とオリジナルとの区別が困難であるという性質があり、情報保全の問題が重要視されている。特に、「コンピュータリソースの共有」，「マルチアクセス」，「広域化」の各要素を満たすコンピュータネットワークの実現が高度情報化社会の確立に不可欠であるが、これは当事者間の情報保全の問題とは矛盾する要素を含んでいる。このような矛盾を解消するための有効な手法として、人類の過去の歴史上主として軍事，外交面で用いられてきた暗号技術が注目されている。

【０００３】

暗号とは、情報の意味が当事者以外には理解できないように情報を交換することである。暗号において、誰でも理解できる元の文（平文）を第三者には意味がわからない文（暗号文）に変換することが暗号化であり、また、暗号文を平文に戻すことが復号であり、この暗号化と復号との全過程をまとめて暗号系と呼ぶ。暗号化の過程及び復号の過程には、それぞれ暗号化鍵及び復号鍵と呼ばれる秘密の情報が用いられる。復号時には秘密の復号鍵が必要であるので、この復号鍵を知っている者のみが暗号文を復号でき、暗号化によって情報の秘密性が維持され得る。

【０００４】

暗号化方式は、大別すると共通鍵暗号系と公開鍵暗号系との二つに分類できる。共通鍵暗号系では、暗号化鍵と復号鍵とが等しく、送信者と受信者とが同じ共通鍵を持つことによって暗号通信を行う。送信者が平文を秘密の共通鍵に基づいて暗号化して受信者に送り、受信者はこの共通鍵を用いて暗号文を平文に復号する。

【０００５】

これに対して公開鍵暗号系では、暗号化鍵と復号鍵とが異なっており、公開されている受信者の公開鍵で送信者が平文を暗号化し、受信者が自身の秘密鍵でその暗号文を復号することによって暗号通信を行う。公開鍵は暗号化のための鍵、秘密鍵は公開鍵によって変換された暗号文を復号するための鍵であり、公開鍵に

よって変換された暗号文は秘密鍵でのみ復号することができる。

【０００６】

公開鍵暗号系の１つの方式として、積和型暗号方式が知られている。これは、送信者である一方のエンティティ側で平文をＫ分割した平文ベクトルｍ＝（m_1，m_2，・・・，m_K）と公開鍵である基数ベクトルｃ＝（c_1，c_2，・・・，c_K）とを用いて、暗号文Ｃ＝m_1 c_1 ＋m_2 c_2 ＋・・・＋m_K c_K を作成し、受信者である他方のエンティティ側でその暗号文Ｃを秘密鍵を用いて平文ベクトルｍに復号して元の平文を得る暗号化方式である。

【０００７】

このような整数環上の演算を利用した積和型暗号に関して、新規な方式及び攻撃法が次々に提案されているが、特に、多くの情報を短時間で処理できるように高速復号可能な暗号化・復号の手法の開発が望まれている。そこで、本発明者等は、中国人の剰余定理を用いることにより、高速な並列復号処理を可能とした積和型暗号における暗号化方法及び復号方法を提案している（特開2000－89669 号）。この暗号化方法は、基数ベクトルｃの成分c_i（ｉ＝１，２，・・・，Ｋ）を、互いに素なＫ個の整数d_iを用いてD_i＝ｄ／d_i（但し、ｄ＝d_1 d_2 ・・・d_K）に設定した基数D_iを基にモジュラ変換したもの、または、互いに素なＫ個の整数d_i，乱数v_i（ｇｃｄ（d_i，v_i）＝１）を用いてV_i＝（ｄ／d_i）v_iに設定した基数V_iを基にモジュラ変換したものにすることを特徴としている。このようにして、中国人の剰余定理を用いて並列に復号するので、高速な復号を行うことができる。

【０００８】

【発明が解決しようとする課題】

しかしながら、この方式では、公開鍵の数を非常に大きくしない限り低密度であるので、ＬＬＬ（Lenstra-Lenstra-Lovasz）アルゴリズムを用いて公開鍵と暗号文とから直接平文を求める低密度攻撃に弱い場合があるという問題があり、安全性の面での更なる改良が望まれている。

【０００９】

本発明は斯かる事情に鑑みてなされたものであり、上記従来例を改良して低密

度攻撃に強く、安全性を向上できる暗号化方法及び復号方法、この暗号化方法を用いる暗号通信方法及び暗号通信システム、並びに、この暗号化方法をコンピュータに実行させるためのコンピュータプログラム及び記録媒体を提供することを目的とする。

【００１０】

【課題を解決するための手段】

請求項１に係る暗号化方法は、平文から暗号文を得る暗号化方法において、暗号化すべき平文を分割してなる複数の成分を有する平文ベクトルに複数の任意の乱数を成分とする乱数ベクトルを加えた合成ベクトルと、公開されている公開ベクトルとを用いて暗号文を得ることを特徴とする。

【００１１】

請求項２に係る暗号化方法は、請求項１において、前記合成ベクトルの成分と前記公開ベクトルの成分との積和演算結果を法で割った剰余を暗号文とすることを特徴とする。

【００１２】

請求項３に係る暗号化方法は、平文から暗号文を得る暗号化方法において、暗号化すべき平文をｋ分割してなるｋ個の成分を有する第１ベクトルにｎ個の任意の乱数を成分とする第２ベクトルを加えた（ｋ＋ｎ）個の成分を有する第３ベクトルと、整数d_i（$1 \leqq i \leqq k+n$）を用いて（ｋ＋ｎ）個の各成分D_iが$D_i = d / d_i$（但し、$d = d_1\ d_2 \cdots d_{k+n}$）に設定された第４ベクトルとを用いて暗号文を得ることを特徴とする。

【００１３】

請求項４に係る暗号化方法は、平文から暗号文を得る暗号化方法において、暗号化すべき平文をｋ分割してなるｋ個の成分を有する第１ベクトルにｎ個の任意の乱数を成分とする第２ベクトルを加えた（ｋ＋ｎ）個の成分を有する第３ベクトルと、整数d_i（$1 \leqq i \leqq k+n$）及び乱数v_iを用いて（ｋ＋ｎ）個の各成分V_iが$V_i = (d / d_i) \cdot v_i$（但し、$d = d_1\ d_2 \cdots d_{k+n}$）に設定された第４ベクトルとを用いて暗号文を得ることを特徴とする。

【００１４】

請求項５に係る暗号化方法は、平文から暗号文を得る暗号化方法において、暗号化すべき平文をｋ分割してなるｋ個の成分を有する第１ベクトルにｎ個の任意の乱数を成分とする第２ベクトルを加えた（ｋ＋ｎ）個の成分を有する第３ベクトルと、Ｌ組（Ｌ≧２）の整数$d_i^{(y)}$（$1 \leqq i \leqq k+n$，$1 \leqq y \leqq L$）を用いて各組毎に（ｋ＋ｎ）個の各成分$D_i^{(y)}$が$D_i^{(y)} = d^{(y)} / d_i^{(y)}$（但し、$d^{(y)} = d_1^{(y)} d_2^{(y)} \cdots d_{k+n}^{(y)}$）に設定されたＬ組の第４ベクトルとを用いて暗号文を得ることを特徴とする。

【００１５】

請求項６に係る暗号化方法は、平文から暗号文を得る暗号化方法において、暗号化すべき平文をｋ分割してなるｋ個の成分を有する第１ベクトルにｎ個の任意の乱数を成分とする第２ベクトルを加えた（ｋ＋ｎ）個の成分を有する第３ベクトルと、Ｌ組（Ｌ≧２）の整数$d_i^{(y)}$（$1 \leqq i \leqq k+n$，$1 \leqq y \leqq L$）及び乱数$v_i^{(y)}$を用いて各組毎に（ｋ＋ｎ）個の各成分$V_i^{(y)}$が$V_i^{(y)} = (d^{(y)} / d_i^{(y)}) \cdot v_i^{(y)}$（但し、$d^{(y)} = d_1^{(y)} d_2^{(y)} \cdots d_{k+n}^{(y)}$）に設定されたＬ組の第４ベクトルとを用いて暗号文を得ることを特徴とする。

【００１６】

請求項７に係る暗号化方法は、請求項４において、$gcd(V_i, d_i) = 1$を満たすことを特徴とする。

【００１７】

請求項８に係る暗号化方法は、請求項６において、$gcd(V_i^{(y)}, d_i^{(y)}) = 1$を満たすことを特徴とする。

【００１８】

請求項９に係る暗号化方法は、請求項６または８において、$gcd(d_i^{(y)}, d_j^{(y)}) = 1$（$1 \leqq j \leqq k+n$）を満たすことを特徴とする。
は８に記載の暗号化方法。

【００１９】

請求項１０に係る暗号化方法は、請求項３～９の何れかにおいて、前記第３ベクトルの各成分と、前記第４ベクトルを基にモジュラ変換した公開鍵ベクトルの各成分とによる積和演算に基づいて暗号文を得るようにしたことを特徴とする。

【００２０】

請求項１１に係る暗号化方法は、平文から暗号文を得る暗号化方法において、暗号化すべき平文を分割してなるｋ個の成分を有する第１ベクトル、ｎ個の任意の乱数を成分とする第２ベクトル、及び、前記ｋ個の成分または前記ｎ個の成分の位置を特定する情報を示すｈ個の成分を有する第３ベクトルを加えたＫ（＝ｋ＋ｎ＋ｈ）個の成分を有する第４ベクトルと、公開されている第５ベクトルとを用いて暗号文を得ることを特徴とする。

【００２１】

請求項１２に係る暗号化方法は、請求項１１において、前記暗号文は、前記第４ベクトルと前記第５ベクトルとを用いて得られる複数のブロックから構成されており、各ブロックにおいて、前記第４ベクトルにおける前記ｈ個の成分の位置は同一であることを特徴とする。

【００２２】

請求項１３に係る暗号化方法は、請求項１１において、前記暗号文は、前記第４ベクトルと前記第５ベクトルとを用いて得られる複数のブロックから構成されており、前のブロックでの前記ｋ個の成分に応じて次のブロックでの前記第４ベクトルにおける前記ｋ個の成分または前記ｎ個の成分の位置を決定することを特徴とする。

【００２３】

請求項１４に係る暗号化方法は、請求項１１において、前記暗号文は、前記第４ベクトルと前記第５ベクトルとを用いて得られる１つのブロックと、前記第３ベクトルのｈ個の成分を平文を分割してなるｈ個の成分に置き換えた前記第４ベクトルと前記第５ベクトルとを用いて得られる複数のブロックとから構成されており、前のブロックでの平文を分割してなる前記ｋ個または（ｋ＋ｈ）個の成分に応じて次のブロックでの前記第４ベクトルにおける（ｋ＋ｈ）個の成分または前記ｎ個の成分の位置を決定することを特徴とする。

【００２４】

請求項１５に係る暗号化方法は、請求項１１～１４の何れかにおいて、前記第５ベクトルは、整数d_i（$1 \leqq i \leqq K$）を用いて各成分D_iがD_i＝（ｄ／d_i

）（但し、$d=d_1\ d_2 \cdots d_K$）に設定された第６ベクトルとを用いて生成することを特徴とする。

【００２５】

請求項１６に係る暗号化方法は、請求項１１～１４の何れかにおいて、前記第５ベクトルは、整数d_i（$1 \leqq i \leqq K$）及び乱数v_iを用いて各成分V_iが$V_i=(d/d_i)\cdot v_i$（但し、$d=d_1\ d_2 \cdots d_K$）に設定された第６ベクトルとを用いて生成することを特徴とする。

【００２６】

請求項１７に係る暗号化方法は、請求項１１～１４の何れかにおいて、前記第５ベクトルは、Ｌ組（$L \geqq 2$）の整数$d_i^{(y)}$（$1 \leqq i \leqq K$，$1 \leqq y \leqq L$）を用いて各組毎にＫ個の各成分$D_i^{(y)}$が$D_i^{(y)}=d^{(y)}/d_i^{(y)}$（但し、$d^{(y)}=d_1^{(y)}\ d_2^{(y)} \cdots d_K^{(y)}$）に設定されたＬ組の第６ベクトルとを用いて生成することを特徴とする。

【００２７】

請求項１８に係る暗号化方法は、請求項１１～１４の何れかにおいて、前記第５ベクトルは、Ｌ組（$L \geqq 2$）の整数$d_i^{(y)}$（$1 \leqq i \leqq k+n$，$1 \leqq y \leqq L$）及び乱数$v_i^{(y)}$を用いて各組毎にＫ個の各成分$V_i^{(y)}$が$V_i^{(y)}=(d^{(y)}/d_i^{(y)})\cdot v_i^{(y)}$（但し、$d^{(y)}=d_1^{(y)}\ d_2^{(y)} \cdots d_K^{(y)}$）に設定されたＬ組の第６ベクトルとを用いて生成することを特徴とする。

【００２８】

請求項１９に係る暗号化方法は、請求項１６において、$gcd(V_i, d_i)=1$を満たすことを特徴とする。

【００２９】

請求項２０に係る暗号化方法は、請求項１８において、$gcd(V_i^{(y)}, d_i^{(y)})=1$を満たすことを特徴とする。

【００３０】

請求項２１に係る暗号化方法は、請求項１８または２０において、$gcd(d_i^{(y)}, d_j^{(y)})=1$（$1 \leqq j \leqq K$）を満たすことを特徴とする。

【００３１】

請求項２２に係る暗号化方法は、請求項１５～２１の何れかにおいて、前記第４ベクトルの各成分と、前記第６ベクトルを基にモジュラ変換した前記第５ベクトルの各成分とによる積和演算に基づいて暗号文を得るようにしたことを特徴とする。

【００３２】

請求項２３に係る復号方法は、請求項１～１０の何れかに記載の暗号化方法を用いて得られた暗号文を復号する復号方法であって、前記平文ベクトルまたは前記第１ベクトルの成分を、前記乱数ベクトルまたは前記第２ベクトルの成分とは独立的に復号することを特徴とする。

【００３３】

請求項２４に係る復号方法は、請求項１～２または１１～２１の何れかに記載の暗号化方法を用いて得られた暗号文を復号する復号方法であって、前記平文ベクトルまたは前記第１ベクトルの成分の位置を同定しながら、前記暗号文を平文に復号することを特徴とする。

【００３４】

請求項２５に係る暗号通信方法は、第１のエンティティ側で、請求項１に記載の暗号化方法に従って平文から暗号文を作成して第２のエンティティ側へ伝送し、伝送された暗号文を該第２のエンティティ側で平文に復号することにより、エンティティ間で情報の通信を行う暗号通信方法であって、前記合成ベクトルにおける前記平文ベクトルの成分または前記乱数ベクトルの成分の位置を前記第１のエンティティ側で設定し、その設定した位置を示す情報を前記第２のエンティティ側へ報知することを特徴とする。

【００３５】

請求項２６に係る暗号通信方法は、請求項２５において、前記設定した位置を示す情報を、作成する暗号文に盛り込んで前記第２のエンティティ側へ伝送することを特徴とする。

【００３６】

請求項２７に係る暗号通信方法は、第１のエンティティ側で、請求項１に記載の暗号化方法に従って平文から暗号文を作成して第２のエンティティ側へ伝送し

、伝送された暗号文を該第２のエンティティ側で平文に復号することにより、エンティティ間で情報の通信を行う暗号通信方法であって、前記合成ベクトルにおける前記平文ベクトルの成分または前記乱数ベクトルの成分の位置を前記第２のエンティティ側で設定し、その設定した位置を示す情報を前記第１のエンティティ側へ報知することを特徴とする。

【００３７】

請求項２８に係る暗号通信システムは、両エンティティ間で暗号文による情報通信を行う暗号通信システムにおいて、請求項１～２２の何れかに記載の暗号化方法を用いて平文から暗号文を作成する暗号化器と、作成した暗号文を第１のエンティティから第２のエンティティへ送信する通信路と、送信された暗号文から平文を復号する復号器とを備えることを特徴とする。

【００３８】

請求項２９に係るコンピュータプログラムは、コンピュータに、平文から積和型の暗号文を得ることを実行させるためのコンピュータプログラムにおいて、暗号化すべき平文を分割してなる複数の成分を有する平文ベクトルに複数の任意の乱数を成分とする乱数ベクトルを加えて合成ベクトルを得る手順と、該合成ベクトルと公開されている公開ベクトルとを用いて暗号文を得る手順とを、コンピュータに実行させることを特徴とする。

【００３９】

請求項３０に係る記録媒体は、コンピュータに、平文から積和型の暗号文を得させるためのコンピュータプログラムを記録してあるコンピュータでの読み取りが可能な記録媒体において、暗号化すべき平文を分割してなる複数の成分を有する平文ベクトルに複数の任意の乱数を成分とする乱数ベクトルを加えた合成ベクトルを得ることをコンピュータに実行させるプログラムコード手段と、該合成ベクトルと公開されている公開ベクトルとを用いて暗号文を得ることをコンピュータに実行させるプログラムコード手段とを含むコンピュータプログラムを記録してあることを特徴とする。

【００４０】

本発明では、平文に冗長性を持たせる、言い換えると平文を退化させて暗号文

を作成する。即ち、暗号化すべき平文を分割してなる平文ベクトルに特に暗号化を必要としない乱数成分からなる乱数ベクトルを付加して合成ベクトルとし、その合成ベクトルと公開されている公開鍵ベクトルとを用いて暗号文を作成する。より具体的には、合成ベクトルの成分と公開ベクトルの成分との積和演算結果、または、その積和演算結果を法で割った剰余を暗号文とする。

【００４１】

本発明では、暗号化が必要でない冗長部分（退化部分）を付加しているため、暗号文の密度が高くなり、また、１つの平文ベクトルに対して非常に多数の合成ベクトルつまり非常に多数の暗号文が存在するので、ＬＬＬアルゴリズムに基づく低密度攻撃は非常に困難となる。この結果、安全性が向上する。

【００４２】

例えば、暗号化すべき平文を分割してなる第１ベクトル（平文ベクトル）及び特に暗号化を必要としない乱数成分からなる第２ベクトル（疑似平文ベクトル）を合わせた第３ベクトル（拡大平文ベクトル）と、各成分を$D_i = d / d_i$ または$V_i = (d / d_i) \cdot v_i$ に設定した１また複数の第４ベクトル（基数ベクトル）とを用いて暗号文を作成する。具体的には、第３ベクトル（拡大平文ベクトル）の各成分と、１また複数の第４ベクトル（基数ベクトル）を基にモジュラ変換した公開鍵ベクトルの各成分との積和演算結果、または、その積和演算結果を法で割った剰余によって暗号文を作成する。

【００４３】

また、本来の暗号化すべき平文部分である平文ベクトルの各成分の位置、または、冗長部分（退化部分）である乱数ベクトルの各成分を付加する位置は、固定でなく、送信側のエンティティまたは受信側のエンティティにて任意に設定できる。このように平文部分の位置または冗長部分（退化部分）の付加位置が固定でなく、任意に設定するため、その位置が攻撃者には未知であるため、安全性は更に向上する。

【００４４】

また、この設定位置を示す情報は、設定した側のエンティティから他方のエンティティへ、公開で伝えても良いし、秘密裏に伝えても良い。送信側のエンティ

ティがこの位置を設定する場合、その設定位置を示す情報は、暗号文に盛り込んで暗号文と共に受信側のエンティティへ送るようにしても良いし、暗号文伝送とは別の経路により受信側のエンティティへ送っても良い。

【００４５】

暗号文に盛り込んで設定位置を示す情報を送る場合、具体的には、暗号化すべき平文を分割してなる第１ベクトル（平文ベクトル）、特に暗号化を必要としない乱数成分からなる第２ベクトル（疑似平文ベクトル）、及び、第１ベクトルまたは第２ベクトルの各成分の位置を示す第３ベクトル（位置特定ベクトル）を合わせた第４ベクトル（伸長平文ベクトル）と、公開されている第５ベクトル（公開鍵ベクトル）とを用いて暗号文を作成する。具体的には、第４ベクトル（伸長平文ベクトル）の各成分と、１または複数の第６ベクトル（基数ベクトル）を基にモジュラ変換した第５ベクトル（公開鍵ベクトル）の各成分との積和演算結果、または、その積和演算結果を法で割った剰余によって暗号文を作成する。この際、第３ベクトルの各成分の位置は公開とする。この位置情報は第３ベクトル（位置特定ベクトル）として暗号文に盛り込まれて、受信側のエンティティへ伝送され、その第３ベクトルの各成分の位置は公開されているので、受信側のエンティティにて、第３ベクトルの成分が復号され、その復号結果に基づき第１ベクトル（平文ベクトル）の各成分の位置が分かって、平文に復号できる。

【００４６】

【発明の実施の形態】

以下、本発明の実施の形態について具体的に説明する。

図１は、本発明による暗号化方法をエンティティａ，ｂ間の情報通信に利用した状態を示す模式図である。図１の例では、一方のエンティティａが、暗号化器１にて平文ｘを暗号文Ｃに暗号化し、通信路３を介してその暗号文Ｃを他方のエンティティｂへ送信し、エンティティｂが、復号器２にてその暗号文Ｃを元の平文ｘに復号する場合を示している。

【００４７】

（第１実施の形態）

秘密鍵と公開鍵とを以下のように準備する。

・秘密鍵：$\{d_i\}$，$\{d_i'\}$，$\{v_i\}$，P，w

・公開鍵：$\{c_i\}$

【００４８】

e＞e′として、正規基数d_i及び退化基数d_i'は、夫々下記（１），（２）を満たす基数と定義する。

【００４９】

【数１】

$$d_i = 2^e + \delta_i \quad (1 \ll \delta_i \ll 2^e) \quad \cdots \quad (1)$$

$$d_i' = 2^{e'} + \delta_i' \quad (1 \ll \delta_i' \ll 2^{e'}) \quad \cdots \quad (2)$$

【００５０】

（k＋n）個の互いに素な数からなる基数を定める。但し、そのうちのi∈Iに対応するk個を正規基数、i∈I′に対応するn個を退化基数とする。ここで、I，I′は何れもインデックス集合であり、I＝｛1，2，…，k｝，I′＝｛k＋1，k＋2，…，k＋n｝とし、I″＝I∪I′とする。なお、第１，第２実施の形態では、特に断らない限り、i∈I″である。次に、基数積D_iを下記（３）に従って求める。

【００５１】

【数２】

$$D_i = \begin{cases} \dfrac{d_1 \cdots d_k d_{k+1}' \cdots d_{k+n}'}{d_i} & (i \in I) \\ \dfrac{d_1 \cdots d_k d_{k+1}' \cdots d_{k+n}'}{d_i'} & (i \in I') \end{cases} \quad \cdots \quad (3)$$

【００５２】

また、（k＋n）個の乱数$\{v_i\}$（但し、gcd（d_i，v_i）＝１）を生成し、変換基数積V_iを下記（４）により導く。

$$V_i = D_i \ v_i \qquad \cdots (4)$$

【００５３】

エンティティａ側で、エンティティｂへ暗号化して送信すべき平文ｘをｋ分割して、各成分がｅ（ビット）である平文ベクトルｇ＝（g_1，g_2，…，g_k）を得る。また、エンティティｂへ特に送信する必要がない各成分がｅ（ビット）の乱数からなる疑似平文ベクトルｇ′＝（g_{k+1}，g_{k+2}，…，g_{k+n}）を得る。例えば、エンティティｂへ特に送信する必要がない平文（冗長文）をｎ分割して、この疑似平文ベクトルｇ′を得ることができる。これらの平文ベクトルｇと疑似平文ベクトルｇ′とを結合して、（ｋ＋ｎ）個の成分を有する拡大平文ベクトルｇ″＝（g_1″，g_2″，…，g_{k+n}″）を得る。ここで、この拡大平文ベクトルｇ″の各成分は、下記（５）のように定義される。

【００５４】

【数３】

$$g_i'' = \begin{cases} g_i & (i \in I) \\ g_i' & (i \in I') \end{cases} \qquad \cdots \quad (5)$$

【００５５】

積和平文Ｍを、拡大平文ベクトルｇ″と変換基数積V_iとを用いて、下記（６）のように定義する。

$$M = g_1'' \ V_1 + g_2'' \ V_2 + \cdots + g_{k+n}'' \ V_{k+n} \qquad \cdots (6)$$

【００５６】

任意の拡大平文ベクトルｇ″に対して、Ｍ＜Ｐを満たす素数Ｐを生成して法とする。素数Ｐより小さい乱数ｗを定め、下記（７）に従って、下記（８）に示すような公開鍵ベクトルｃを導いて公開する。

$$c_i \equiv w V_i \pmod{P} \qquad \cdots (7)$$

$$\text{ベクトル}c = (c_1, c_2, \cdots, c_{k+n}) \qquad \cdots (8)$$

【００５７】

エンティティａ側で、拡大平文ベクトルｇ″と公開鍵ベクトルｃとの内積を下

記（９）のように求めて、暗号文Ｃを得る。作成された暗号文Ｃは通信路３を介してエンティティａからエンティティｂへ送信される。

$$C=g_1'' c_1+g_2'' c_2+\cdots+g_{k+n}'' c_{k+n} \quad \cdots(9)$$

【００５８】

エンティティｂ側では、以下のようにして復号処理が行われる。

暗号文Ｃから積和平文Ｍは、下記（10）のようにして求めることができる。

$$M\equiv w^{-1}C \pmod{P} \quad \cdots(10)$$

【００５９】

拡大平文ベクトルｇ″のうち、正規基数に対応するインデックス、即ち、ｉ∈Ｉに関しては、下記（11）が成立して、平文ベクトルｇを復号することができる。

$$g_i\equiv MV_i^{-1} \pmod{d_i} \quad \cdots(11)$$

【００６０】

なお、退化基数に対応するインデックス、即ち、ｉ∈Ｉ′に関しては、復号する必要がない。また、上記（11）と同様に下記（12）に従って復号しようとしても、退化の影響によりビット数に関して下記（13）の関係があるので、疑似平文ベクトルｇ′を正しく復号することはできない。

$$g_i''' \equiv MV_i^{-1} \pmod{d_i'} \quad \cdots(12)$$

$$g_i' > d_i' > g_i''' \quad \cdots(13)$$

【００６１】

なお、上記例では、ｇｃｄ（V_i，d_i）＝１としたが、ｇｃｄ（V_i，d_i）＝A_iとしても良い。この場合には、$V_i'=V_i/A_i$，$d_i'=d_i/A_i$とおいて、ｇｃｄ（V_i'，d_i'）＝１として同様に行えば良い。また、上記例では、基数積D_iに乱数｛v_i｝を付加するようにしたが、このような乱数を付加せず、上記（３）で示される基数積D_iをそのまま用いても良い。

【００６２】

（第２実施の形態）

秘密鍵と公開鍵とを以下のように準備する。

・秘密鍵：｛$d_i^{(P)}$｝，｛$d_i^{(Q)}$｝，｛$d_i^{(P)\prime}$｝，｛$d_i^{(Q)\prime}$｝，

$\{v_i^{(P)}\}$，$\{v_i^{(Q)}\}$，P，Q，N，w

・公開鍵：$\{c_i\}$

なお、上記Nは公開であっても良い。

【００６３】

P，Qを後述の条件を満たす素数とする。e＞e′とし、正規基数$d_i^{(P)}$，$d_i^{(Q)}$及び退化基数$d_i^{(P)}$′，$d_i^{(Q)}$′は、夫々下記（14），（15）を満たす基数と定義する。

【００６４】

【数４】

$$d_i^{(P)} d_i^{(Q)} = 2^e + \delta_i \quad (1 \ll \delta_i \ll 2^e) \quad \cdots \quad (14)$$

$$d_i^{(P)'} d_i^{(Q)'} = 2^{e'} + \delta_i' \quad (1 \ll \delta_i' \ll 2^{e'}) \quad \cdots \quad (15)$$

【００６５】

法P及び法Qについて、夫々第１実施の形態と同様に、２組の基数$\{d_i^{(P)}\}$，$\{d_i^{(P)}{}'\}$及び$\{d_i^{(Q)}\}$，$\{d_i^{(Q)}{}'\}$（但し、i≠jにおいて、$\gcd(d_i^{(P)}, d_j^{(P)}) = 1$，$\gcd(d_i^{(Q)}, d_j^{(Q)}) = 1$）を生成する。但し、任意のi∈I″について、下記（16），（17）を満たすものとする。

$$\gcd(d_i^{(P)}, d_i^{(Q)}) = 1 \quad \cdots (16)$$

$$\gcd(d_i^{(P)}{}', d_i^{(Q)}{}') = 1 \quad \cdots (17)$$

【００６６】

次に、法P及び法Qについて、第１実施の形態と同様に、２組の乱数$\{v_i^{(P)}\}$及び$\{v_i^{(Q)}\}$（但し、$\gcd(d_i^{(P)}, v_i^{(P)}) = 1$，$\gcd(d_i^{(Q)}, v_i^{(Q)}) = 1$）を生成し、上記（３），（４）と同様の計算により、$\{V_i^{(P)}\}$及び$\{V_i^{(Q)}\}$を導く。

【００６７】

第１実施の形態と全く同様に構成された拡大平文ベクトルg″に対する法P及び法Qにおける積和平文M_P及び積和平文M_Qを夫々、下記（18），（19）と定義する。

$$M_P = g_1 \prime\, V_1^{(P)} + g_2 \prime\, V_2^{(P)} + \cdots + g_{k+n} \prime\, V_{k+n}^{(P)} \quad \cdots (18)$$

$$M_Q = g_1 \prime\, V_1^{(Q)} + g_2 \prime\, V_2^{(Q)} + \cdots + g_{k+n} \prime\, V_{k+n}^{(Q)} \quad \cdots (19)$$

【００６８】

更に、素数Ｐ及び素数Ｑを、任意の拡大平文ベクトルｇ″に対してM_P＜ＰかつM_Q＜Ｑの条件を満たすように生成し、それらの積をＮとする。中国人の剰余定理を用いて、Ｐ及びＱによる余りが夫々$V_1^{(P)}$及び$V_1^{(Q)}$となるような最小の$V_1^{(N)}$（＜Ｎ）を導いて変換基数積と定義する。

【００６９】

積和平文Ｍを、拡大平文ベクトルｇ″と変換基数積$V_1^{(N)}$とを用いて、下記（20）のように定義する。ここで、Ｍ＜Ｎを満たす必要はない。

$$M = g_1 \prime\, V_1^{(N)} + g_2 \prime\, V_2^{(N)} + \cdots + g_{k+n} \prime\, V_{k+n}^{(N)} \quad \cdots (20)$$

【００７０】

Ｎより小さい乱数ｗを定め、下記（21）に従って、下記（22）に示すような公開鍵ベクトルｃを導いて公開する。

$$c_i \equiv w V_i \pmod N \quad \cdots (21)$$

$$\text{ベクトル}c = (c_1, c_2, \cdots, c_{k+n}) \quad \cdots (22)$$

【００７１】

エンティティａ側で、拡大平文ベクトルｇ″と公開鍵ベクトルｃとの内積を下記（23）のように求めて、暗号文Ｃを得る。作成された暗号文Ｃは通信路３を介してエンティティａからエンティティｂへ送信される。なお、Ｎを公開する場合には、下記（23）のＣをＮで割った剰余を暗号文とすれば良い。

$$C = g_1 \prime\, c_1 + g_2 \prime\, c_2 + \cdots + g_{k+n} \prime\, c_{k+n} \quad \cdots (23)$$

【００７２】

エンティティｂ側では、以下のようにして復号処理が行われる。

積和平文Ｍは、下記（24）を満たす。従って、法Ｐ及び法Ｑにおける積和平文M_P及びM_Qは、下記（25），（26）のようにして求めることができる。

$$M \equiv w^{-1} C \pmod{N} \quad \cdots (24)$$

$$M_P \equiv M \pmod{P} \quad \cdots (25)$$

$$M_Q \equiv M \pmod{Q} \quad \cdots (26)$$

【００７３】

拡大平文ベクトルｇ″のうち、正規基数に対応するインデックス、即ち、ｉ∈Ｉに関しては、$2^e < d_i^{(P)} d_i^{(Q)}$であるため、下記（27），（28）によって（$g_i^{(P)}$，$g_i^{(Q)}$）を求め、中国人の剰余定理を適用することにより、下記（29）が成立して、平文ベクトルｇを復号することができる。

【００７４】

【数５】

$$g_i^{(P)} \equiv M_P V_i^{(P)-1} \pmod{d_i^{(P)}} \quad \cdots (27)$$

$$g_i^{(Q)} \equiv M_Q V_i^{(Q)-1} \pmod{d_i^{(Q)}} \quad \cdots (28)$$

$$g_i \equiv \begin{cases} g_i^{(P)} \pmod{d_i^{(P)}} \\ g_i^{(Q)} \pmod{d_i^{(Q)}} \end{cases} \quad \cdots (29)$$

【００７５】

なお、退化基数に対応するインデックス、即ち、ｉ∈Ｉ′に関しては、第１実施の形態と同様、復号する必要がなく、疑似平文ベクトルｇ′を正しく復号することができない。

【００７６】

なお、上記例では、２組の基数｛$d_i^{(P)}$｝，｛$d_i^{(Q)}$｝に乱数｛$v_i^{(P)}$｝，｛$v_i^{(Q)}$｝を付加するようにしたが、このような乱数を付加しない基数積を使用しても良い。

【００７７】

次に、上述したような第１，第２実施の形態の方式にあって、ＬＬＬアルゴリズムに基づく低密度攻撃に強い耐性を持てるように、１を超える高い密度を実現できていることを説明する。退化していない一般的な積和型暗号について、暗号

文密度σ，方式密度ρ，レートηを下記（30），（31），（32）のように定義する。なお、Ｃは暗号文のビット数，C_{max} は取り得る最大の暗号文のビット数，ｋは平文の分割数，ｅは分割平文のビット数である。

【００７８】

【数６】

$$\sigma = \frac{\sum_{i=1}^{k} \log_2 g_i}{\log_2 C} \quad \cdots \quad (30)$$

$$\rho = \frac{k e}{\log_2 C_{max}} \quad \cdots \quad (31)$$

$$\eta = \frac{k e}{|C_{max}|} \quad \cdots \quad (32)$$

【００７９】

また、第１，第２実施の形態のように退化している積和型暗号について、暗号文密度σ′，方式密度ρ′を下記（33），（34）のように定義する。なお、レートは上記（32）と同じである。

【００８０】

【数７】

$$\sigma' = \frac{\sum_{i=1}^{k+n} \log_2 g_i''}{\log_2 C} \quad \cdots \quad (33)$$

$$\rho' = \frac{(k+n)\, e}{\log_2 C_{max}} \quad \cdots \quad (34)$$

【００８１】

第１実施の形態における密度について考察する。乱数 v_i をｓビットとする。

密度をできる限り大きくするために、取り得る最大の積和平文をM_{max}とした場合、法Ｐのビットサイズを｜Ｐ｜＝｜M_{max}｜と設定すべきである。この場合、第１実施の形態における方式密度ρ_1，レートη_1は、夫々、下記（35），（36）の条件を満たす。

【００８２】

【数８】

$$\rho_1 = \frac{(k+n)\,e}{e+\log_2 P+\log_2 (k+n)} > \frac{(k+n)\,e}{(k+2)\,e+(n-1)\,e'+s+2\log_2 (k+n)+1} \quad \cdots (35)$$

$$\eta_1 = \frac{k\,e}{e+\log_2 P+\log_2 (k+n)} > \frac{k\,e}{(k+2)\,e+(n-1)\,e'+s+2\log_2 (k+n)+1} \quad \cdots (36)$$

【００８３】

公開鍵より秘密鍵を求める攻撃（片柳磨子，村上恭通，笠原正雄：”積和型暗号に関する二，三の考察”，1999年暗号と情報セキュリティシンポジウム資料，Ｂ43 Jan.2000 に開示）を回避するためには、乱数v_iのビットサイズを法Ｐのビットサイズの１／４以上にする必要がある。この条件を満たすように、乱数v_iのビットサイズを$s=(1/4)\log_2 P+1$と考えて計算した場合、方式密度ρ_1，レートη_1は、夫々、下記（37），（38）の条件を満たす。

【００８４】

【数９】

$$\rho_1 > \frac{3(k+n)e}{(4k+7)e+4(n-1)e'+7\log_2(k+n)+7} \quad \cdots (37)$$

$$\eta_1 > \frac{3ke}{(4k+7)e+4(n-1)e'+7\log_2(k+n)+7} \quad \cdots (38)$$

【００８５】

この条件において、乱数v_iが非常に大きいので、e′をe′＜e／２とする、または、k＜nとすることにより、$\rho_1 > 1$を満たすパラメータが存在する。

【００８６】

第２実施の形態における密度について考察する。乱数$v_i^{(P)}$と$v_i^{(Q)}$との積、即ち、$v_i^{(P)} v_i^{(Q)}$をｓビットとする。法Ｎが非公開である場合、密度をできる限り大きくするために、取り得る最大の積和平文をM_{Pmax}, M_{Qmax}としたとき、｜Ｐ｜＝｜M_{Pmax}｜，｜Ｑ｜＝｜M_{Qmax}｜と設定すべきである。この場合、第２実施の形態における方式密度ρ_2，レートη_2は、夫々、下記（39），（40）の条件を満たす。

【００８７】

【数１０】

$$\rho_2 = \frac{(k+n)\,e}{e+\log_2 N+\log_2 (k+n)}$$

$$> \frac{(k+n)\,e}{(k+3)\,e+(n-1)\,e'+s+3\log_2 (k+n)+1} \quad \cdots (39)$$

$$\eta_2 = \frac{k\,e}{e+\log_2 N+\log_2 (k+n)}$$

$$> \frac{K\,e}{(k+3)\,e+(n-1)\,e'+s+3\log_2 (k+n)+1} \quad \cdots (40)$$

【００８８】

第２実施の形態では、多重化しているので、乱数をあまり大きくする必要はない。よって、ｅ′＝ｅ／２，ｋ＝ｎという条件であっても、容易に方式密度ρ_2＞１，レートη_2＞１／２を達成することができる。例えば、上記の条件において、分割数をｋ＝８とし、基数$d_i^{(P)}$，$d_i^{(Q)}$及び乱数$v_i^{(P)}$，$v_i^{(Q)}$を何れも３２ビットとした場合、ρ_2＝1.0174，η_2＝0.5087となり、このような小さなパラメータでも、上記の条件（ρ_2＞１，η_2＞１／２）を実現できている。但し、小さなパラメータでは安全性に問題があるので、例えばｋ＝１００，ｅ＝６４，ｅ′＝３２程度が現実的である。

【００８９】

また、法Ｎを公開とし、ＣをＮで割った剰余を暗号文とした場合の第２実施の形態における方式密度ρ_2，レートη_2は、夫々、下記（41），（42）の条件を満たす。

【００９０】

【数１１】

$$\rho_2 = \frac{(k+n)\,e}{\log_2 N}$$

$$> \frac{(k+n)\,e}{(k+2)\,e + (n-1)\,e' + s + 2\log_2 (k+n) + 1} \quad \cdots (41)$$

$$\eta_2 = \frac{k\,e}{\log_2 N}$$

$$> \frac{k\,e}{(k+2)\,e + (n-1)\,e' + s + 2\log_2 (k+n) + 1} \quad \cdots (42)$$

【００９１】

以上のように、法Ｎを公開とした場合には、法Ｎが非公開である場合に比べて、方式密度ρ_2，レートη_2の何れもが向上している。

【００９２】

ところで、疑似平文ベクトルｇ′における乱数成分は、平文ベクトルｇとは全く独立して設定できる。よって、作成した暗号文Ｃの方式密度が高くなるように疑似平文ベクトルｇ′の乱数成分を設定するようにすれば良い。また、疑似平文ベクトルｇ′としてある乱数系列を設定して暗号文Ｃを作成した後、その暗号文Ｃの方式密度を計算し、その計算値が１を超えない場合には、疑似平文ベクトルｇ′に設定する乱数系列を別なものにして暗号文Ｃを作成しなおすようにし、方式密度が１を超えた場合の暗号文Ｃを受信先のエンティティへ送信する手法が有効である。

【００９３】

上述した第１，第２実施の形態の方式では、エンティティｂへ特に暗号化して送信する必要がない疑似平文ベクトルの各乱数の拡大平文ベクトルにおける位置（退化位置）は受信側のエンティティｂにて固定的に設定されており、その位置

を表す情報が公開されている。

【００９４】

これに対して、そのような乱数成分の位置（退化位置）、または逆に暗号化すべき平文ベクトルの各成分の位置（正規位置）を、任意に設定できるようにすれば、より安全性が向上することを期待できる。以下の第３実施の形態では、このような退化位置または正規位置を受信側のエンティティａにて任意に設定して、その位置を表す情報を暗号文に盛り込んでエンティティｂへ伝送する場合について説明する。

【００９５】

（第３実施の形態）

まず、第３実施の形態の説明に用いる幾つかの定義について説明する。第３実施の形態にあっても、暗号化すべき平文は幾つかの分割平文に分けられる。各分割平文をメッセージベクトルｍとして扱う。以下に定義する伸長変換によって、メッセージベクトルｍはベクトルｍ′に伸長される。このベクトルｍ′を、伸長メッセージベクトルと称する。これらのベクトルｍ，ベクトルｍ′の各成分のビットサイズの和を夫々ε（ビット），ε′（ビット）（但し、ε≦ε′）とする。また、暗号文が取り得る最大ビット数をC_{max}とする。

【００９６】

〈定義１（密度）〉

方式密度ρを下記（43）のように定義する。

【００９７】

【数１２】

$$\rho = \frac{\varepsilon'}{\log_2 C_{max}} \quad \cdots \quad (43)$$

【００９８】

〈定義２（レート）〉

レートηを下記（44）のように定義する。

【００９９】

【数１３】

$$\eta = \frac{\varepsilon}{|C_{max}|} \quad \cdots \quad (44)$$

【０１００】

ベクトルａ＝（a_1，a_2，・・・，a_w）をｗ次元ベクトルとし、ベクトルｃ＝（c_1，c_2，・・・，c_n）をｎ次元ベクトルとする。また、ベクトルｂ＝（b_1，b_2，・・・，b_n）を重みｗのｎ次元２値ベクトルとする。但し、下記（45）の条件を満たす。

【０１０１】

【数１４】

$$\left.\begin{array}{l} b_{i_1} = b_{i_2} = \cdots = b_{i_w} = 1 \\ i_1 < i_2 < \cdots < i_w \end{array}\right\} \quad \cdots \quad (45)$$

【０１０２】

〈定義３（添数集合）〉

添数集合Ｉ＝Ｉｎｄ（ベクトルｂ）を下記（46）のように定義する。

$$I = \{i_1, i_2, \cdots, i_w\} \quad \cdots (46)$$

【０１０３】

〈定義４（ベクトル表現）〉

添数集合Ｉは、｛１，２，・・・，ｎ｝の部分集合であり、ベクトル表現として、ベクトルｄ＝Ｖｅｃ（Ｉ，ｎ）を下記（47）のように定義する。但し、ベクトルｄ＝（d_1，d_2，・・・，d_n）であり、例えば、Ｉ＝Ｉｎｄ（ベクトルｂ）である場合に、ベクトルｂ＝Ｖｅｃ（Ｉ，ｎ）である。

【０１０４】

【数１５】

$$d_i = \begin{cases} 1 & (i \in I) \\ 0 & (i \notin I) \end{cases} \quad \cdots \quad (47)$$

【０１０５】

〈定義５（伸長）〉

ベクトルｂによりベクトルａから伸長されたｎ次元ベクトルｃは、ベクトルｃ＝ベクトルａ｛ベクトルｂ｝にて表記し、下記（48）のように定義する。例えば、ベクトルａ＝（a_1，a_2，a_3），ベクトルｂ＝（１，０，１，１）である場合に、ベクトルａ｛ベクトルｂ｝＝（a_1，０，a_2，a_3）となる。

【０１０６】

【数１６】

$$\begin{cases} c_{ij} = a_j & \\ c_k = 0 \quad (b_k = 0 \text{ の場合}) & \end{cases} \quad \cdots \quad (48)$$

$$(j = 1, 2, \cdots, w \ 、\ k = 1, 2, \cdots, n)$$

【０１０７】

〈定義６（抜き出し）〉

ベクトルｂによりベクトルｃから抜き出されたｗ次元ベクトルａは、ベクトルａ＝ベクトルｃ｛ベクトルｂ｝にて表記し、下記（49）のように定義する。例えば、ベクトルｃ＝（c_1，c_2，c_3，c_4），ベクトルｂ＝（１，０，１，１）である場合に、第１，第３及び第４成分が抜き出されて、ベクトルｃ｛ベクトルｂ｝＝（c_1，c_3，c_4）となる。

【０１０８】

【数１７】

$$\vec{a} = (c_{i_1}, c_{i_2}, \cdots, c_{iw}) \quad \cdots \quad (49)$$

【０１０９】

次に、第３実施の形態の具体的な方式について説明する。

〈平文分割〉

平文ｘは、ｅｋビットの複数のブロックに分割される。各ブロックは下記（50）のようにメッセージベクトルｍで表現される。なお、m_i（ｉ＝１，２，・・・，ｋ）はｅビットの整数である。

ベクトルｍ＝（m_1，m_2，・・・，m_k）　　…（50）

【０１１０】

〈伸長変換〉

メッセージベクトルｍを、各成分がｅビットの整数であるｋ次元ベクトルとし、乱数ベクトルｒを、各成分がｅ′ビットの整数であるｎ次元ベクトルとする。但し、ｅ＜ｅ′とする。また、ベクトルｓを、重みｋの（ｋ＋ｎ）次元の２値ベクトルとする。このベクトルｓを「位置特定子」と称する。

【０１１１】

ｈを下記（51）のように設定し、ベクトルｓ′を（ｈｅ－（ｋ＋ｎ））ビットの任意の２値詰め物ベクトルとする。ｈｅ次元の２値連接ベクトル［ベクトルｓ｜ベクトルｓ′］は、各成分がｅビットの整数である下記（52）のようなｈ次元のベクトルｔに分割できる。

【０１１２】

【数１８】

$$h = \lceil (k+n) / e \rceil \quad \cdots \quad (51)$$

$$\vec{t} = (t_1, t_2, \cdots, t_h) \quad \cdots \quad (52)$$

【０１１３】

Ｋ＝ｋ＋ｎ＋ｈとし、各添数集合I_N，I_R及びI_Lを夫々下記（53），（54）及び（55）のように定義する。但し、バーベクトルｓはベクトルｓのビット補数を表す。

【０１１４】

【数１９】

$$I_N = Ind(\vec{s}) \quad \cdots (53)$$

$$I_R = Ind(\overline{\vec{s}}) \quad \cdots (54)$$

$$I_L = \{k+n+1,\ k+n+2,\ \cdots,\ K\} \quad \cdots (55)$$

【０１１５】

なお、上記例では添数集合I_Lの成分を最後尾のｈ個としたが、これらの成分の位置は任意であって良い。このような場合、下記（56），（57）の条件を満たし、ベクトルｍ′，ベクトルｓは夫々下記（58），（59）のように表される。

【０１１６】

【数２０】

$$I_N \cup I_R \cup I_L = \{1,\ 2,\ \cdots,\ K\} \quad \cdots (56)$$

$$I_N \cap I_R = I_R \cap I_L = I_L \cap I_N = \phi \quad \cdots (57)$$

$$\vec{m}' = \vec{m}\{Vec(I_N, K)\} + \vec{r}\{Vec(I_R, K)\} + \vec{t}\{Vec(I_L, K)\} \quad \cdots (58)$$

$$\vec{s} = Vec(I_N, K)\ [\overline{Vec(I_L, K)}] \quad \cdots (59)$$

【０１１７】

メッセージベクトルｍを、下記（60）のように、伸長メッセージベクトルｍ′＝（m_1′，m_2′，・・・，m_K′）に変換する。この際、このベクトルｍ′の各成分の大きさは下記（61）である。

【０１１８】

【数２１】

$$\vec{m'} = [\vec{m}\ \{\vec{s}\} + \vec{r}\ \{\vec{s}\}\ |\vec{t}] \quad \cdots \quad (60)$$

$$|m_i'| = \begin{cases} e & (i \in I_N \cup I_L) \\ e' & (i \in I_R) \end{cases} \quad \cdots \quad (61)$$

【０１１９】

〈鍵生成〉

秘密鍵と公開鍵とを以下のように準備する。

・秘密鍵：$\{d_i^{(P)}\}$，$\{d_i^{(Q)}\}$，$\{v_i^{(P)}\}$，$\{v_i^{(Q)}\}$，
P，Q，N，w（但し、i＝1，2，・・・，K）

・公開鍵：ベクトルc＝（c_1，c_2，・・・，c_K），I_L，e，e′

なお、上記Nは公開であっても良い。

【０１２０】

まず、任意のi，j（但し、i≠j）について、下記（62）～（65）の条件を満たすような２組の基数$\{d_i^{(P)}\}$，$\{d_i^{(Q)}\}$を生成する。

【０１２１】

【数２２】

$$gcd(d_i^{(P)}, d_j^{(P)}) = 1 \quad \cdots \quad (62)$$

$$gcd(d_i^{(Q)}, d_j^{(Q)}) = 1 \quad \cdots \quad (63)$$

$$gcd(d_i^{(P)}, d_i^{(Q)}) = 1 \quad \cdots \quad (64)$$

$$d_i^{(P)} d_i^{(Q)} = 2^e + \delta_i \quad (1 \ll \delta_i \ll 2^e) \quad \cdots \quad (65)$$

【０１２２】

$v_i^{(P)}$，$v_i^{(Q)}$をランダムな整数として、下記（66），（67）のように、$V_i^{(P)}$，$V_i^{(Q)}$を導く。但し、$v_i^{(P)}$及び$v_i^{(Q)}$は、下記（68）及び（69）の条件を満たす。

【０１２３】

【数２３】

$$V_i^{(P)} = \frac{d_1^{(P)} d_2^{(P)} \cdots d_k^{(P)}}{d_i^{(P)}} v_i^{(P)} \quad \cdots \quad (66)$$

$$V_i^{(Q)} = \frac{d_1^{(Q)} d_2^{(Q)} \cdots d_k^{(Q)}}{d_i^{(Q)}} v_i^{(Q)} \quad \cdots \quad (67)$$

$$gcd(d_i^{(P)}, v_i^{(P)}) = 1 \quad \cdots \quad (68)$$

$$gcd(d_i^{(Q)}, v_i^{(Q)}) = 1 \quad \cdots \quad (69)$$

【０１２４】

次に、任意の伸長メッセージベクトルm′について条件$M_P < P$，$M_Q < Q$を満たすような大きな素数Ｐ，Ｑを設定する。なお、M_P，M_Qは夫々下記（70），（71）で定義される。

【０１２５】

【数２４】

$$M_P = m'_1 V_1^{(P)} + m'_2 V_2^{(P)} + \cdots + m'_K V_K^{(P)} \quad \cdots \quad (70)$$

$$M_Q = m'_1 V_1^{(Q)} + m'_2 V_2^{(Q)} + \cdots + m'_K V_K^{(Q)} \quad \cdots \quad (71)$$

【０１２６】

そして、Ｎ＝ＰＱを設定し、中国人の剰余定理によりV_i（$0 \leqq V_i < N$）を下記（72）により計算する。

【０１２７】

【数２５】

$$V_i \equiv \begin{cases} V_i^{(P)} \pmod{P} \\ V_i^{(Q)} \pmod{Q} \end{cases} \quad \cdots \quad (72)$$

【０１２８】

公開鍵ベクトルｃの各成分を、下記（73）により求める。ここでｗは、Z_N^*から任意に選ばれた乱数である。

$$c_i \equiv w V_i \pmod{N} \qquad \cdots (73)$$

【０１２９】

〈暗号化〉

エンティティａ側（送信側）で、前述した位置特定子であるベクトルｓを任意に生成する。即ち、メッセージベクトルｍに関する位置を示す添数集合I_Nを、送信者であるエンティティａは任意に選択する。次に、エンティティａ側（送信側）で、各成分が任意に選択されたｅ′ビットの整数からなるｎ次元のベクトルｒを生成する。この乱数ベクトルｒにより、高密度が実現される。つまり、冗長部分（退化部分）である乱数ベクトルｒの付加によって、後述するように密度が高くなる。

【０１３０】

エンティティａ側（送信側）で、メッセージベクトルｍを、ベクトルｓ及びベクトルｒによって、伸長メッセージベクトルｍ′に変換する。そして、この伸長メッセージベクトルｍ′と公開鍵ベクトルｃとの内積を下記（74）のように求めて、暗号文Ｃを得る。作成された暗号文Ｃは通信路３を介してエンティティａからエンティティｂへ送信される。

【０１３１】

【数２６】

$$C = \vec{m'} \cdot \vec{c} = m'_1 c_1 + m'_2 c_2 + \cdots + m'_K c_K \quad \cdots (74)$$

【０１３２】

この暗号化にあっては、暗号化すべき平文を分割したメッセージベクトルｍは、添数集合I_Nにて示される位置で伝送され、添数集合I_Nの情報は、添数集合I_Lにて示される位置でベクトルｓによって伝送される。

【０１３３】

〈復号〉

エンティティｂ側（受信側）で、以下のようにして復号処理が行われる。

中間メッセージMは、下記（75）を満たす。従って、法Ｐ，法Ｑにおける中間メッセージM_P，M_Qは、下記（76），（77）のようにして求めることができる。

$$M \equiv w^{-1}C \pmod{N} \quad \cdots (75)$$

$$M_P \equiv M \pmod{P} \quad \cdots (76)$$

$$M_Q \equiv M \pmod{Q} \quad \cdots (77)$$

【０１３４】

そして、下記（78），（79）によって（$m_i^{(P)}$，$m_i^{(Q)}$）を求め、中国人の剰余定理を適用することにより、下記（80）が成立して、メッセージベクトル$m'' = (m_1'', m_2'', \cdots, m_K'')$を復号することができる。

【０１３５】

【数２７】

$$m_i^{(P)} \equiv M_P V_i^{(P)-1} \pmod{d_i^{(P)}} \quad \cdots (78)$$

$$m_i^{(Q)} \equiv M_Q V_i^{(Q)-1} \pmod{d_i^{(Q)}} \quad \cdots (79)$$

$$m_i'' \equiv \begin{cases} m_i^{(P)} \pmod{d_i^{(P)}} \\ m_i^{(Q)} \pmod{d_i^{(Q)}} \end{cases} \quad \cdots (80)$$

【０１３６】

e′＞eであるので、復号されたメッセージベクトルm″の各成分は、上記（61）から、下記（81）の条件を満たす。

【０１３７】

【数２８】

$$\begin{cases} m_i'' = m_i' & (i \in I_N \cup I_L) \\ m_i'' \neq m_i' & (i \in I_R) \end{cases} \quad \cdots \quad (81)$$

【０１３８】

添数集合I_Lに従って、下記（82）のように、復号ベクトルm″からベクトルｔを取り出す。

【０１３９】

【数２９】

$$\vec{t} = \vec{m''}\,[Vec\,(I_L, K)] \quad \cdots \quad (82)$$

【０１４０】

ベクトルｔをｈｅ次元の２値ベクトル［ベクトルｓ｜ベクトルｓ′］と見なすことにより、（ｋ＋ｎ）次元で重みｋの２値ベクトルｓをエンティティｂ側（受信側）で再構築できる。よって、最終的に、下記（83）のように、メッセージベクトルｍを得ることができる。

【０１４１】

【数３０】

$$\vec{m} = \vec{m''}\,[\vec{s}] \quad \cdots \quad (83)$$

【０１４２】

なお、添数集合I_Lの成分を任意とする一般的な場合には、上記（83）において、ベクトルm″を下記（84）に示すものに代えることにより、メッセージベクトルｍが得られる。

【０１４３】

【数３１】

$$\vec{m''}\,\overline{[Vec\,(I_L, K)]} \quad \cdots \quad (84)$$

【０１４４】

次に、上述したような第３実施の形態の暗号化方式における安全性について述べる。密度が0.9408より小さい場合に、積和型公開鍵暗号はＬＬＬアルゴリズムに基づく低密度攻撃によって破られることが知られている。上述した第３実施の形態の暗号化方式では、１を超える高い密度を実現できており、このことはこの方式が低密度攻撃に対して安全であることを示している。

【０１４５】

乱数$v_i^{(P)}$，$v_i^{(Q)}$を何れもｆビットとした場合、上述した第３実施の形態の暗号化方式における密度ρは、下記（85）の条件を満たす。但し、Ｋ＝ｋ＋ｎ＋ｈ，ｅ′＞ｅである。

【０１４６】

【数３２】

$$\rho > \frac{(k+h)\,e+ne'}{e'+\log_2 N+\log_2 n} > \frac{Ke+n\,(e'-e)}{Ke+(3e'-e)+f+1+3\log_2 n} \quad \cdots \quad (85)$$

【０１４７】

例えば、ここで簡単のために、ｆ＝ｅ，ｅ′＝２ｅと設定した場合、ｎは下記（86）の条件を満たすので、ρ＞１を実現できている。現実的な例として、ｅ＝32とした場合、何れのｋについてもｎ＝７とすることにより、ρ＞１を達成できることが分かる。

【０１４８】

【数３３】

$$(n-6)\,e>3\log_2 n+1 \quad \cdots \quad (86)$$

【０１４９】

また、第３実施の形態の暗号化方式では、高いレートも実現できている。上述した本発明の暗号化方式におけるレートηは、下記（87）の条件を満たす。

【０１５０】

【数３４】

$$\eta = \frac{ke}{\lceil e' + \log_2 N + \log_2 n \rceil} > \frac{ke}{Ke + (3e' - e) + f + 1 + 3\log_2 n} \quad \cdots (87)$$

【０１５１】

ここで簡単のために、ｆ＝ｅ，ｅ′＝２ｅと設定した場合、ｎ及びｋは下記（88）の条件を満たすので、$\eta > 0.5$ を実現できている。現実的な例として、ｅ＝32とした場合、ｎ＝７でｋ＞14とすることにより、$\eta > 0.5$ を達成できることが分かる。例えば、ｋ＝57とした場合に、$\eta \fallingdotseq 0.7884$となる。このように、レートの観点から見ても、第３実施の形態の方式は効率的である。

【０１５２】

【数３５】

$$\left(k - n - \left\lceil \frac{k+n}{e} \right\rceil - 6\right) e > 3\log_2 n + 1 \quad \cdots (88)$$

【０１５３】

第３実施の形態の暗号化方式では、高い密度を実現できるため、低密度攻撃に対し、十分に安全である。また、送信側のエンティティにおいて、退化基数の位置を自由に決定できる。よって、位置が分かっている退化基数に基づき、攻撃者が第３実施の形態の暗号化方式に対して有効な攻撃を行おうとした場合でも、その攻撃者にとって退化基数の位置を同定することが困難である。従って、退化基数の位置が固定ではなく送信側で任意に決定できるという第３実施の形態の特徴は、退化基数の位置が既知である場合に有効である攻撃に対しても安全であることを示している。

【０１５４】

以下、第３実施の形態の他の例について説明する。上述した例では全てのブロ

ックにおいて、I_Lの位置を固定（最後尾）としているが、このI_Lの位置は各ブロックにおいて異なっていても良い。このような例として、以下のようなものが可能である。

【０１５５】

（第１例）

最初のブロックについてはI_Lの位置を固定（例えば上述した例と同様に最後尾）し、このI_Lは公開しておく。そして、２番目以降のブロックについては、１つ前のブロックのメッセージベクトルよりそのブロックのI_Lの位置を決定するようにする。よって、２番目以降のブロックからは、I_Lの位置が変動する。このようにして、送信側のエンティティが退化基数の位置を任意に決定しても最初のブロックのI_Lは公開されており、しかも、２番目以降のブロックでは前のブロックのメッセージベクトルからそのブロックのI_Lの位置が分かるので、受信側のエンティティにおいて、上述した例と同様に、暗号文から平文を復号できる。この第１例では、各ブロックにおいてI_Lの位置を変動させるため、安全性の向上を図れる。

【０１５６】

（第２例）

最初のブロックについてはI_Lの位置を固定（例えば上述した例と同様に最後尾）し、このI_Lは公開しておく。そして、２番目以降のブロックについては、I_Lの項を設けないようにし、I_Lの項に割り当てられるｈ次元のベクトルを平文を分割したメッセージに割り当てる。そして、この２番目以降のブロックについては、１つ前のブロックのメッセージよりそのブロックにおける退化基数の位置を示す位置情報を決定する。よって、２番目以降のブロックには、I_Lが存在しない。このようにして、送信側のエンティティが退化基数の位置を任意に決定しても最初のブロックのI_Lは公開されており、しかも、２番目以降のブロックでは前のブロックのメッセージベクトルからそのブロックでの退化基数の位置が分かるので、受信側のエンティティにおいて、上述した例と同様に、暗号文から平文を復号できる。また、２番目以降のブロックではメッセージに割り当てる部分がｋ項から（ｋ＋ｈ）項に増えるので、１ブロック内に盛り込めるメッセージ

量が増加して、レートをより高くすることができる。

【０１５７】

なお、上記例では、暗号化すべき平文を分割したメッセージベクトルｍの各成分の位置（添数集合I_N）を示す情報（添数集合I_L）を伝送するようにしたが、付加する乱数ベクトルｒの各成分の位置（添数集合I_R）を示す情報を伝送するようにしても良いことは勿論である。

【０１５８】

また、上記例では、２組の基数$\{d_i^{(P)}\}$，$\{d_i^{(Q)}\}$に乱数$\{v_i^{(P)}\}$，$\{v_i^{(Q)}\}$を付加するようにしたが、このような乱数を付加しない基数積を使用しても良い。

【０１５９】

また、上記例では（74）に示したように、伸長メッセージベクトルｍ′と公開鍵ベクトルｃとの内積値（積和演算結果）をそのまま暗号文Ｃとしたが、下記（89）のように、その内積値（積和演算結果）をＮでモジュロ変換したもの、つまり上記（74）のＣをＮで割った剰余を暗号文としても良い。

$$C \equiv m_1' c_1 + m_2' c_2 + \cdots + m_K' c_K \pmod{N} \quad \cdots (89)$$

【０１６０】

（74）のように暗号文を表す場合に、安全性の根拠は、下記（90）に示す式において、a_1，a_2，…，a_n及びＣが既知の整数であるときに未知数x_1，x_2，…，x_nを求めるための線型ジオファンタス方程式を解くことの困難さに基づいている。一方、（89）のように暗号文を表す場合には、積和してモジュロをとるので、安全性の根拠がＮの素因素分解の困難さに基づいている。この場合、Ｎを公開するので攻撃者に提供する情報量は増えるが、積和演算結果そのものでなくてその余りしか分からないので、線型ジオファンタス方程式を解く難しさは高くなっている。

$$C = a_1 x_1 + a_2 x_2 + \cdots + a_n x_n \quad \cdots (90)$$

【０１６１】

（第４実施の形態）

なお、第３実施の形態では、送信側のエンティティにて任意に設定した、伸長

メッセージベクトルにおけるメッセージベクトルの各成分または乱数ベクトルの各成分の位置を示す情報を暗号文に盛り込むようにしたが、このような位置を示す情報を、暗号文との伝送とは独立させて、送信側のエンティティから受信側のエンティティへ報せるようにしても良い。

【０１６２】

（第５実施の形態）

なお、第３，第４実施の形態では、送信側のエンティティにて伸長メッセージベクトルにおけるメッセージベクトルの各成分または乱数ベクトルの各成分の位置を任意に設定するようにしたが、このような位置を受信側のエンティティにて任意に設定するようにすることも可能である。

【０１６３】

（第６実施の形態）

また、第３～第５実施の形態では、Ｋ個の要素からなる基数の集合｛d_i｝を２組（｛$d_i^{(P)}$｝，｛$d_i^{(Q)}$｝）生成する多重化した方式の場合について説明したが、前述した第１実施の形態のように１組の基数の集合｛d_i｝を用いる方式についても、これらの第３～第５実施の形態を同様に適用できることは勿論である。

【０１６４】

図２は、本発明の記録媒体の実施の形態の構成を示す図である。ここに例示するコンピュータプログラムは、上述した暗号化方式の手順に従って拡大平文ベクトルｇ″または伸長メッセージベクトルｍ′を得る処理と、得た拡大平文ベクトルｇ″または伸長メッセージベクトルｍ′と公開鍵ベクトルｃとの内積計算により暗号文Ｃを作成する処理とを含んでおり、以下に説明する記録媒体に記録されている。なお、コンピュータ10は、送信側のエンティティに設けられている。

【０１６５】

図２において、コンピュータ10とオンライン接続する記録媒体11は、コンピュータ10の設置場所から隔たって設置される例えばＷＷＷ(World Wide Web)のサーバコンピュータを用いてなり、記録媒体11には前述の如きプログラム11a が記録されている。記録媒体11から通信線等の伝送媒体14を介して読み出されたプログ

ラム11a がコンピュータ10を制御することにより、コンピュータ10が暗号文Ｃを作成する。

【０１６６】

コンピュータ10の内部に設けられた記録媒体12は、内蔵設置される例えばハードディスクドライブまたはＲＯＭなどを用いてなり、記録媒体12には前述の如きプログラム12a が記録されている。記録媒体12から読み出されたプログラム12a がコンピュータ10を制御することにより、コンピュータ10が暗号文Ｃを作成する。

【０１６７】

コンピュータ10に設けられたディスクドライブ10a に装填して使用される記録媒体13は、運搬可能な例えば光磁気ディスク，ＣＤ－ＲＯＭまたはフレキシブルディスクなどを用いてなり、記録媒体13には前述の如きプログラム13a が記録されている。記録媒体13から読み出されたプログラム13a がコンピュータ10を制御することにより、コンピュータ10が暗号文Ｃを作成する。

【０１６８】

【発明の効果】

以上のように、本発明では、暗号化すべき平文を分割してなる平文ベクトルに、複数の任意の乱数を成分とする乱数ベクトルを加えた合成ベクトルと、公開されている公開ベクトルとを用いて暗号文を得るようにしたので、暗号化が必要でない乱数からなる冗長部分（退化部分）を付加しているため、暗号文の密度を大きくでき、ＬＬＬアルゴリズムに基づく低密度攻撃に対して強くなって安全性を向上できる。また、その合成ベクトルにおける平文ベクトルまたは乱数ベクトルの各成分の位置を、送信側のエンティティまたは受信側のエンティティにて任意設定できるようにしたので、攻撃者にとってその位置を見つけることすら困難であり、安全性の更なる向上を図れる。この結果、積和型暗号の実用化の道を開くことに、本発明は大いに寄与できる。

【図面の簡単な説明】

【図１】

２人のエンティティ間における情報の通信状態を示す模式図である。

【図２】

記録媒体の実施の形態の構成を示す図である。

【符号の説明】

１　暗号化器

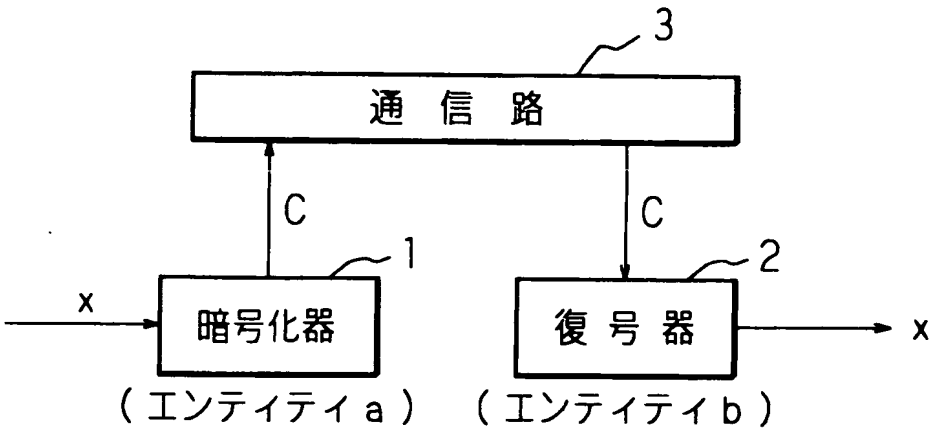
２　復号器

３　通信路

ａ，ｂ　エンティティ

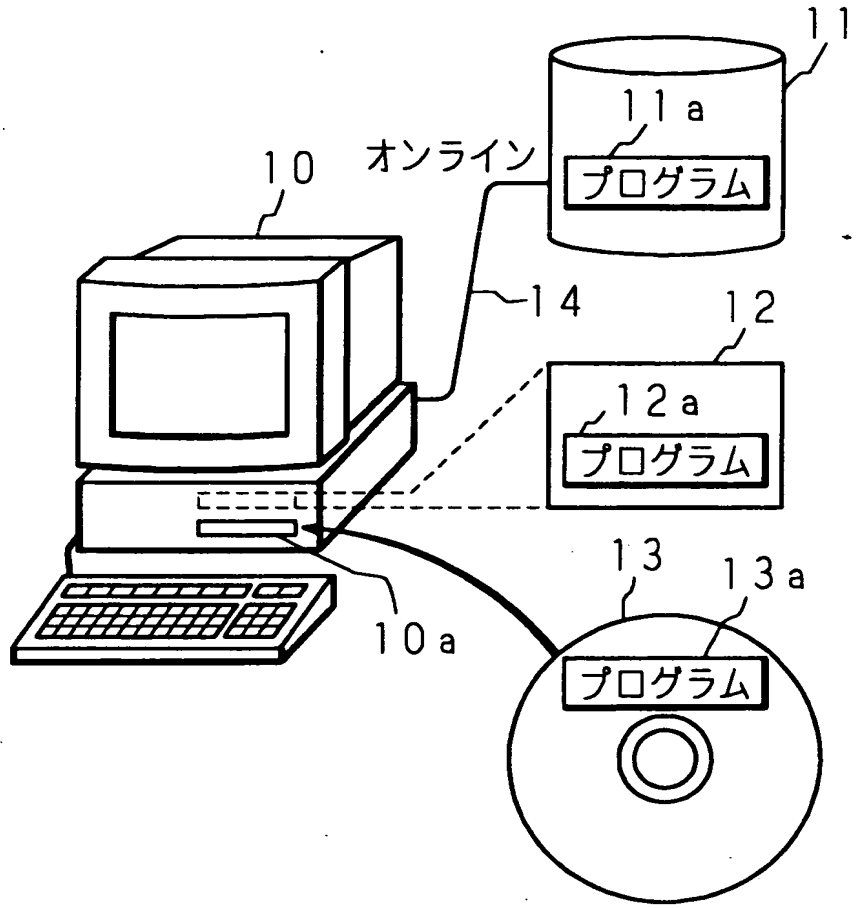
【書類名】　　図面

【図１】



出証特２００１－３０４０４９１

【図２】



【書類名】　　要約書

【要約】

【課題】　ＬＬＬアルゴリズムに基づく低密度攻撃に強く、安全性を向上できる暗号化方式を提供する。

【解決手段】　暗号化すべき平文を分割した平文ベクトルに任意の乱数成分からなる乱数ベクトルを加えた合成ベクトルの各成分と、１または複数組の整数d_i（$1 \leqq i \leqq K$）及び乱数v_iを用いて$V_i = (d / d_i) \cdot v_i$（但し、$d = d_1\ d_2 \cdots d_K$（任意の２つの整数$d_i$，$d_j$は互いに素））に設定された１または複数の基数ベクトルを基にモジュラ変換した公開鍵ベクトルの各成分との積和演算により暗号文Ｃを得る。合成ベクトルにおける平文ベクトルまたは乱数ベクトルの各成分の位置は、送信側（エンティティａ）または受信側（エンティティｂ）で任意に設定する。

【選択図】　　図１

出　願　人　履　歴　情　報

識別番号　　〔０００００６２９７〕

１．変更年月日　　１９９０年　８月　７日
［変更理由］　新規登録
住　所　京都府京都市南区吉祥院南落合町３番地
氏　名　村田機械株式会社

出　願　人　履　歴　情　報

識別番号　　〔５９７００８６３６〕

１．変更年月日　　１９９７年　１月２１日
［変更理由］　新規登録
住　所　　大阪府箕面市粟生外院４丁目１５番３号
氏　名　　笠原　正雄